CARLSON LYNCH

SCOTT + SCOTT

+ Via ECF +

August 12, 2019

The Honorable Thomas W. Thrash, Jr.
Chief United States District Judge
Northern District of Georgia
Richard B. Russell Building
75 Ted Turner Drive, S.W.
Atlanta, GA 30303

Re: *In Re: Equifax, Inc. Customer Data Security Breach Litigation*
MDL No. 2800 (N.D. Ga.)

Dear Judge Thrash:

Plaintiffs seek an order requiring Equifax to produce certain documents that it has made available through a restricted "reading room." As set forth below, the reading room impermissibly restricts Plaintiffs' ability to prosecute their claims and forces Plaintiffs to disclose privileged work product by requiring Plaintiffs to both code documents on a system controlled and managed by Equifax's counsel and disclose who can access such documents, including potential experts and consultants.

Equifax claims that certain documents are so sensitive that Plaintiffs' counsel cannot host and review them in an unredacted form on Plaintiffs' own document review platform. Plaintiffs are keenly aware of their responsibility to protect confidential information. The protective order already entered in this action provides the necessary protection for Equifax (and other parties that produce confidential information), and Plaintiffs, in selecting a discovery vendor, were conscious of the need for enhanced protection. To avoid this dispute, Plaintiffs proposed implementing stringent safeguards, such as, among others, multi-factor authentication and limiting access to select individuals, to further protect documents that would otherwise have been produced in the reading room. Equifax refused to agree to Plaintiffs' proposals or explain why Plaintiffs – as officers of the Court – cannot be trusted to securely handle confidential information. No court overseeing a data breach action has ever ordered the onerous restrictions Equifax seeks to impose on Plaintiffs, and no reason exists for this Court to be the first.

Background

On April 4, 2018, the Court entered a Protective Order governing the handling of "Highly Confidential Information," the disclosure of which "would create a substantial risk of serious harm that could not be avoided by less restrictive means." (ECF No. 298 §II.C.) Such Highly Confidential Information can only be provided to a limited subset of specifically identified individuals "to the extent reasonably necessary" to prosecute Plaintiffs' claims. (*Id.* §V.C.)

On February 27, 2019, Equifax, for the first time, informed Plaintiffs that, because it believed some documents were so sensitive, Equifax would not provide access to them outside of a reading room that Equifax established, and which it manages through its discovery vendor, Deloitte Touche Tohamatsu Ltd. ("Deloitte"). The reading room prohibits Plaintiffs from printing, downloading, or otherwise sharing documents amongst themselves. Plaintiffs cannot add document reviewers or coding tags, batch out documents for review, or generate reports without Deloitte's assistance. Plaintiffs cannot copy or paste ***any*** information to or from the reading room, including information that plainly isn't sensitive, such as the Bates numbers of potentially relevant documents.

Compounding the burden on Plaintiffs, Equifax has produced redacted versions of documents interred in the Reading Room for Plaintiffs to review on Plaintiffs' document review platform. Equifax does not utilize the same bates numbers between such documents. Plaintiffs thus have a duplicative, unredacted set of documents in the Reading Room, and a redacted set on Plaintiffs' system.

Although Equifax initially produced nearly 25,000 documents to Plaintiffs through the Reading Room, after Plaintiffs' identified many documents that did not contain "sensitive" information, including some that were ***publicly available***, Equifax agreed to remove approximately 21,000 documents and produce them to Plaintiffs in the normal course.

Recognizing that the reading room is unsanctioned under the terms of the Protective Order, Equifax has proposed amendments to govern the handling of purportedly "Restricted Highly Sensitive Information" ("RHSI") that will further stymie Plaintiffs' ability to use such documents.[1] Equifax asks the Court to prohibit

[1] The reading room also violates the parties' ESI Protocol, ECF No. 449, which Equifax has not proposed to further amend.

Plaintiffs from: copying or recording RHSI; printing more than 250 pages of documents containing RHSI; making more than three copies of any printed document – and then, only if Plaintiffs maintain a log identifying the document copied and number of copies of made; storing documents containing RHSI on a "network of any kind," including firm intranets; allowing secretaries to handle documents containing RHSI; and, regardless of the number of experts designated or consultants retained, sharing documents containing RHSI with more than two experts or consultants, whose identity Plaintiffs would have to disclose to Equifax. Notably, Equifax has never confirmed that its own attorneys are subject to these proposed restrictions.

Plaintiffs offered to negotiate additional protections that would apply to Plaintiffs' own document review platform. These include implementing dual-factor authentication; segregating documents containing RHSI; limiting access to select users designated by Plaintiffs' counsel; and allowing Equifax to verify that such measures have been implemented. Equifax never responded to Plaintiffs' proposal.

Equifax's primary justification for its onerous restrictions is merely that the risk of improper disclosure increases the more persons have access to RHSI. Such reasoning cannot justify the limitations Equifax seeks to impose on Plaintiffs.

Argument

I. No Court Overseeing a Data Breach Case Has Ever Endorsed the Onerous Restrictions Equifax Seeks to Impose on Plaintiffs

The cases Equifax cited to Plaintiffs in its correspondence do not support the establishment of a reading room.[2] Specifically, Equifax has cited patent infringement and trade secret cases that constrain litigants who are direct competitors. *See, e.g.*, *St. Jude Med., Inc. v. Intermedics, Inc.*, 107 F.R.D. 398, 400 (D. Minn. 1985) (trade secret misappropriation case between two manufacturers of heart valve components); *Brown Bag Software v. Symantec Corp.*, 960 F.2d 1465, 1470 (9th Cir. 1992) (trade secret misappropriation action); *Safe Flight Instrument Corp. v. Sundstrand Data Control Inc.*, 682 F. Supp. 20, 21 (D. Del. 1988) (restricting Plaintiff's President, a competitor, from examining discovery material in light of "his human ability during future years of research to separate the applications he has extrapolated from Sundstrand's documents from those he develops from his own ideas"); T*ailored*

[2] Should the Court so desire, Plaintiffs and Equifax can jointly submit their prior correspondence regarding the dispute.

Lighting, Inc. v. Osram Sylvania Prod., Inc., 236 F.R.D. 146, 147 (W.D.N.Y. 2006) (entering protective order because "unfettered access to proprietary information by principals and employees of the requesting party puts the disclosing party at great risk of suffering a competitive injury if the proprietary information which is disclosed is used or exploited, even subconsciously, by the requesting party"); *Protegrity Corp. v. Epicor Software Corp.*, No. 3:13 CV 1781 JBA, 2014 WL 3864899, at *3 (D. Conn. Aug. 6, 2014) (patent infringement action); *GeoTag, Inc. v. Frontier Commc'ns Corp.*, No. 2:10-CV-569, 2013 WL 12134192 (E.D. Tex. Jan. 8, 2013) (same). Such cases merely stand for the proposition that heightened protections may be warranted where litigants have a market incentive to violate protective orders.

No such concerns are present here. Rather than have any competitive interest in the material Equifax seeks to protect, Plaintiffs and Plaintiffs' counsel share the same vested interest as Equifax to ensure that confidential information remains confidential to prevent another data breach of Plaintiffs' PII and PCD. Indeed, Plaintiffs have alleged that "if another breach at Equifax occurs," it is Plaintiffs, and not just Equifax, who would "suffer irreparable harm" in the form of "reputational harm and the loss of goodwill" from Plaintiffs' own customers. FAC ¶610.

Moreover, the materials Equifax seeks to designate as RHSI, such as "penetration test results/reports, [and] vulnerability scan results/reports," are routinely requested and produced in data breach litigation. Plaintiffs' experts and consultants will rely upon such documents in proving Equifax's negligence. "[B]ecause all attorneys are officers of the court, 'the general rule is that attorneys operating under a protective order will properly handle confidential information.'" *Alza Corp. v. Impax Labs.*, Inc., No. C-03-4032, 2004 WL 7339748, at *2 (N.D. Cal. June 21, 2004) (citation omitted). That is why Plaintiffs are aware of no court overseeing data breach litigation that has ever ordered the onerous restrictions Equifax seeks to impose on Plaintiffs.

II. Equifax's Proposals Would Result in a *Per Se* Handover of Plaintiffs' Privileged Work Product

Plaintiffs further object to the reading room because it would require Plaintiffs to tell Equifax who seeks access to such documents, which documents they wish to review, and would force Plaintiffs to review, code, and tag documents on an Equifax-controlled system.

"Not even the most liberal of discovery theories can justify unwarranted inquiries into the files and the mental impressions of an attorney." *Hickman v. Taylor*, 329 US 495, 510 (1947). It is uncontroversial that the work product privilege protects an attorney's "mental impressions," *Johnson v. Gross*, 611 F. App'x 544, 547 (11th Cir. 2015), but also protects an attorney's "searches, filters, document review, coding and tagging of documents," which are "not available to any other party." *Bombardier Recreational Prod., Inc. v. Arctic Cat, Inc.*, No. 12-CV-2706, 2014 WL 10714011, at *15 (D. Minn. Dec. 5, 2014).

Equifax claims that the Deloitte personnel supporting Equifax will have no access to the work product Plaintiffs entrust to the reading room. Such an argument misses the point. The "[d]enial or grant of access" to privileged or confidential information "cannot rest on a general assumption that one group of lawyers are more likely or less likely inadvertently to breach their duty under a protective order." *U.S. Steel Corp. v. United States*, 730 F.2d 1465, 1468 (Fed. Cir. 1984). It is fundamentally unfair for Equifax to claim that Plaintiffs' counsel cannot be trusted to secure confidential materials while, at the same time, asking Plaintiffs to trust that Equifax and its vendor will not make use of Plaintiffs' privileged work product.

Plaintiffs have proposed a less burdensome, and more reasonable proposal that would require them to implement multi-factor authentication and limit who can access such documents. Plaintiffs' selected vendor – Driven, Inc. – is a leading eDiscovery vendor and has agreed to host any data produced in the litigation in a secure data center and follow all applicable industry security standards. Equifax has failed to explain why Plaintiffs' proposals would not be sufficient to achieve the security sought while still protecting Plaintiffs' work product.

Conclusion

For the foregoing reasons, Plaintiffs respectfully request that the Court reject Equifax's reading room and order Equifax's to produce documents in the reading room to plaintiffs following implementation of the safeguards Plaintiffs propose.

Sincerely,

/s/ Joseph P. Guglielmo

SCOTT+SCOTT,
ATTORNEYS AT LAW, LLP

/s/ Gary F. Lynch

CARLSON LYNCH, LLP

Joseph P. Guglielmo
The Helmsley Building
230 Park Ave., 17th Floor
New York, NY 10169
Telephone: (212) 223-4478
jguglielmo@scott-scott.com

Gary F. Lynch
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Telephone: (412) 322-9243
glynch@carlsonlynch.com